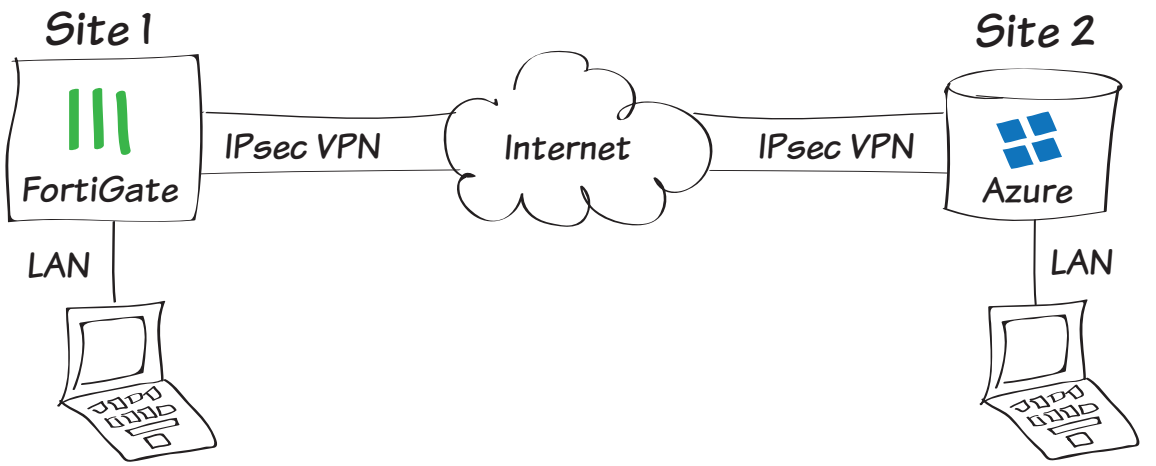
# Configuring IPsec VPN between a FortiGate and Microsoft Azure™

The following recipe describes how to configure a site-to-site IPsec VPN tunnel. In this example, one site is behind a FortiGate and another site is hosted on Microsoft Azure™, for which you will need a valid Microsoft Azure profile.

Using FortiOS 5.2, the example demonstrates how to configure the tunnel between each site, avoiding overlapping subnets, so that a secure tunnel can be established with the desired security profiles applied.

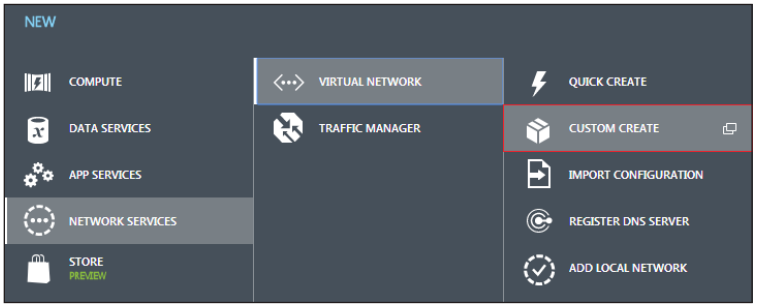
1. Configuring the Microsoft Azure™ virtual network
2. Creating the Microsoft Azure™ virtual network gateway
3. Configuring the FortiGate tunnel
4. Creating the FortiGate firewall addresses
5. Creating the FortiGate firewall policies
6. Results



## 1. Configuring the Microsoft Azure™ virtual network

Log into Microsoft Azure and click **New** in the lower-left corner to add a new service.


From the prompt, select **Network Services** > **Virtual Network** > **Custom Create**.




Under 'Virtual Network Details', enter a **Name** for the VPN and a **Location** where you want the VMs to reside, then click the **Next** arrow.

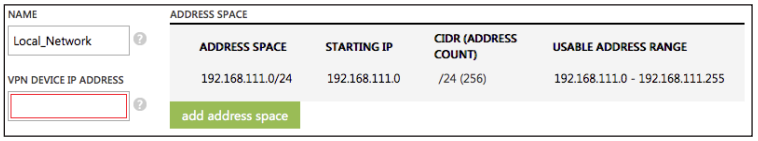

Under 'DNS Servers and VPN Connectivity', enable the **Configure a site-to-site VPN** checkbox and enter DNS server information if required.

Click the **Next** arrow.


Under 'Site-to-Site Connectivity', enter a **Name** and **IP Address** for the FortiGate device.

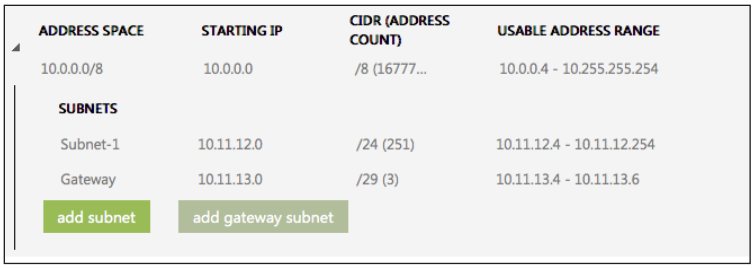
Under Address Space, include a **Starting IP** and **CIDR (Address Count)** for the tunnel, avoiding overlapping subnets.

Click the **Next** arrow.

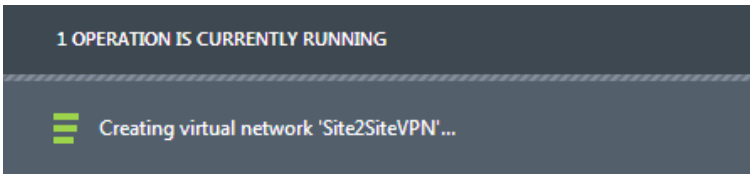


Under ‘Virtual Network Address Spaces’, configure the desired address space or accept the default settings.

Select **add gateway subnet** to configure a gateway IP and click the **Checkmark** in the lower-right corner to accept the configuration.

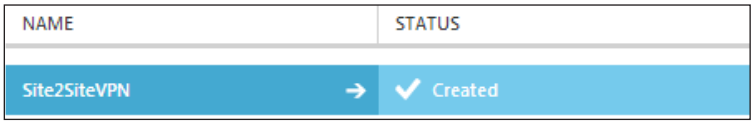



After accepting the configuration, you will have to wait a short period of time for the virtual network to be created, but it shouldn’t be long.

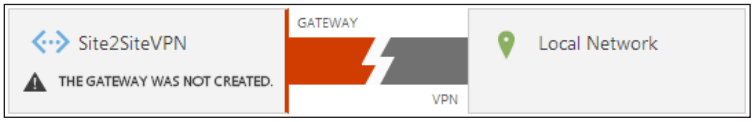



## 2. Creating the Microsoft Azure™ virtual network gateway

On the ‘networks’ home screen, click the name of the virtual network you just created.

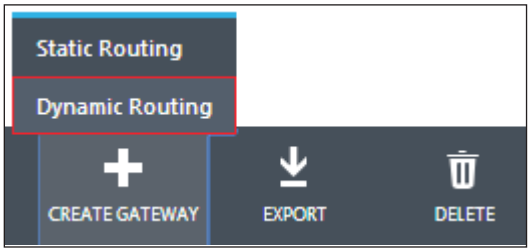



Under this virtual network, go to the **Dashboard**. You will notice that the gateway has not yet been created. You will create the gateway in this step.

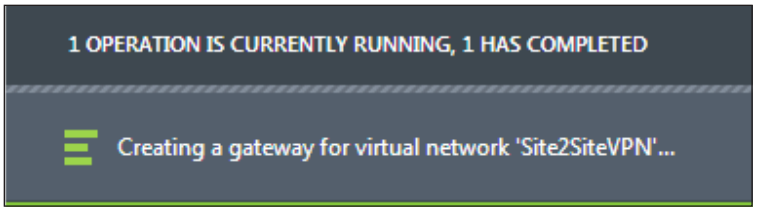



At the bottom of the screen, select **Create Gateway** > **Dynamic Routing**.

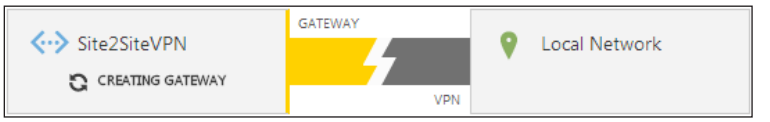
When prompted, select **Yes**.



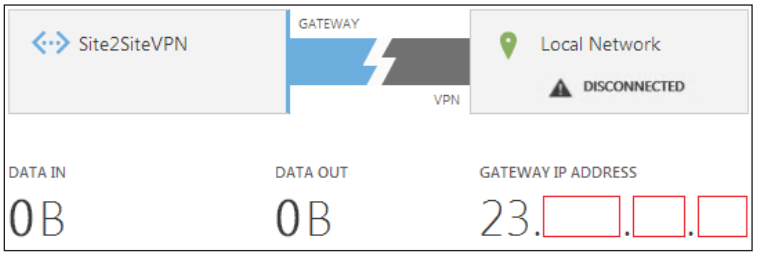
The operation to create the virtual network gateway will run. The process takes a short amount of time.



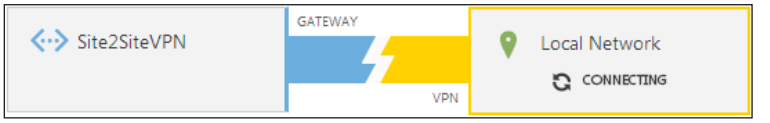

Azure will indicate to you that the gateway is being created. You may wish to leave this running for a few minutes as wait periods in excess of 10 minutes are common.




When the operation is complete, the status changes and you are given a **Gateway IP Address**.



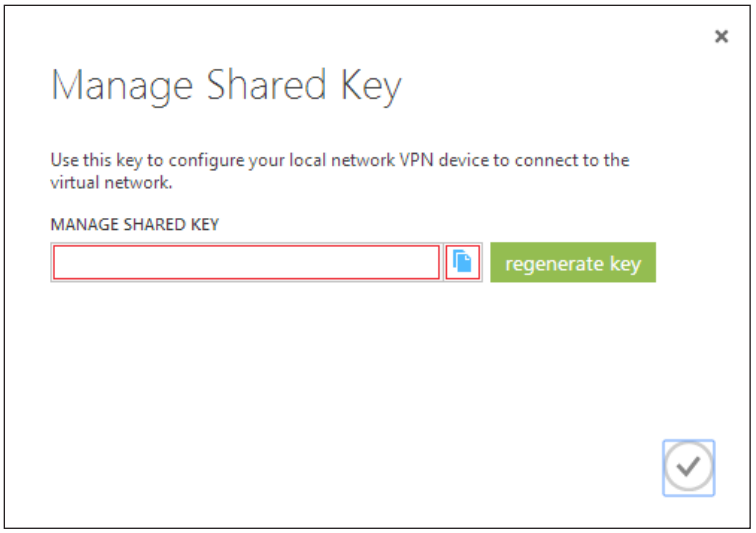

The gateway will then attempt to connect to the Local Network.




At the bottom of the screen, select **Manage Key**.

The ‘Manage Shared Key’ dialogue appears. **Copy** the key that is shown. You can select **regenerate key** if you want to copy a different key.

Click the **Checkmark** when you are confident that the key is copied.

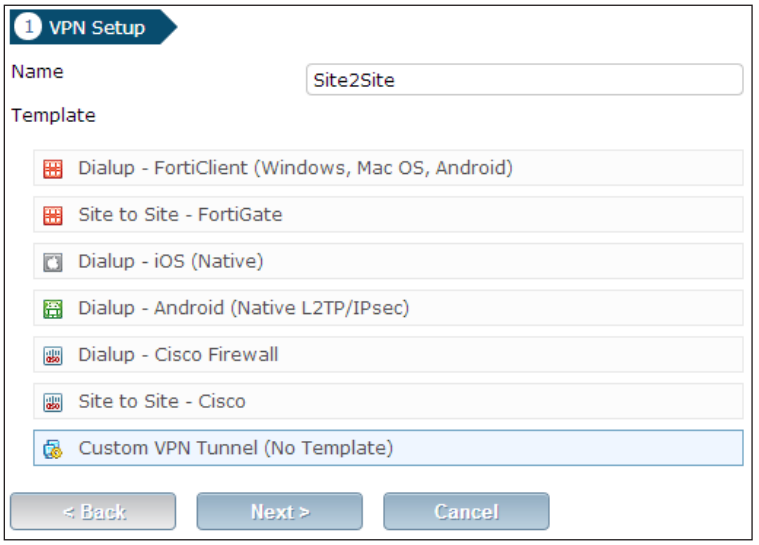



You are now ready to configure the FortiGate endpoint of the tunnel.

## 3. Configuring the FortiGate tunnel

Go to **VPN** > **IPsec** > **Wizard** and select **Custom VPN Tunnel (No Template)**.

Enter a **Name** for the tunnel and click **Next**.

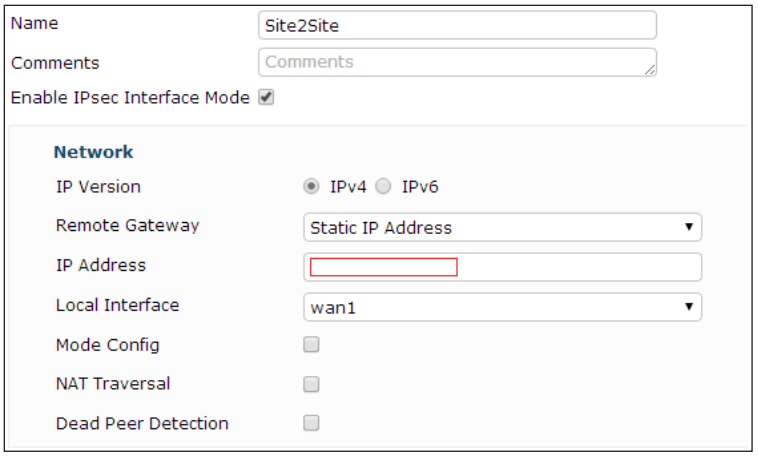


Enter the desired parameters. Set the **Remote Gateway** to **Static IP Address**, and include the gateway **IP Address** provided by Microsoft Azure.

Set the **Local Interface** to **wan1**.

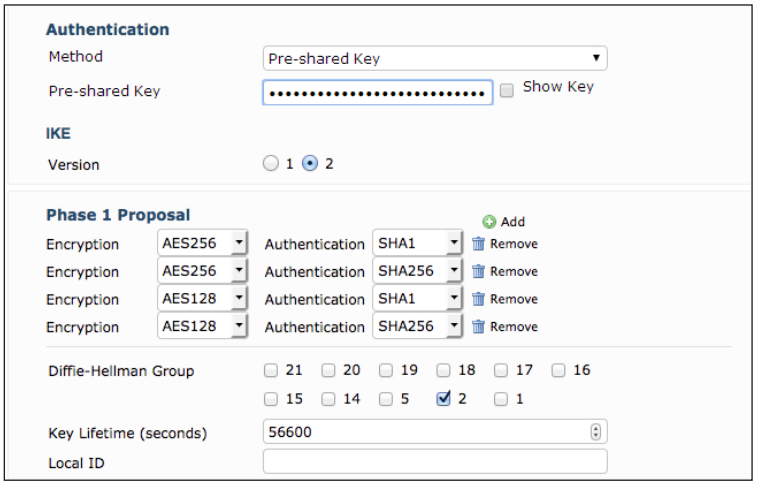
Under **Authentication**, enter the **Pre-shared Key** provided by Microsoft Azure.

Disable **NAT Traversal** and **Dead Peer Detection**.



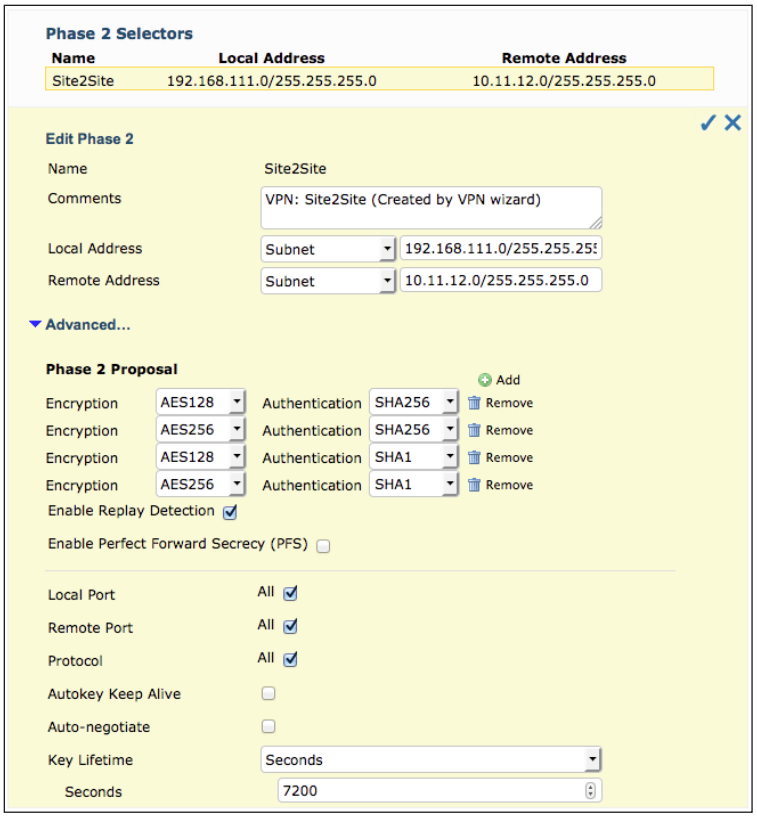

Under **Authentication**, ensure that you enable **IKEv2** and set **DH Group** to **2**.

Enable the encryption types shown and set the **Keylife** to **56600** seconds.



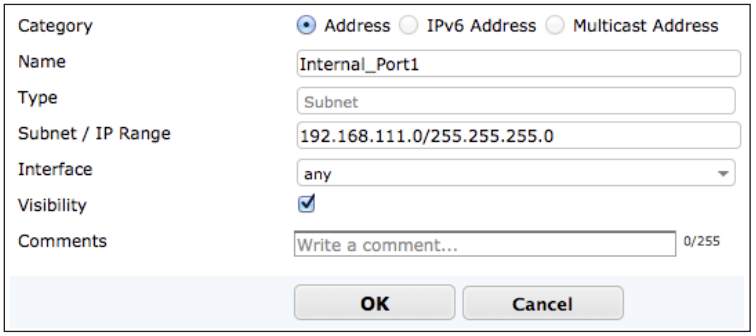
Scroll down to **Phase 2 Selectors** and set **Local Address** to the local subnet and **Remote Address** to the VPN tunnel endpoint subnet (found under 'Virtual Network Address Spaces' in Microsoft Azure).

Enable the encryption types to match Phase 1 and set the **Keylife** to **7200** seconds.

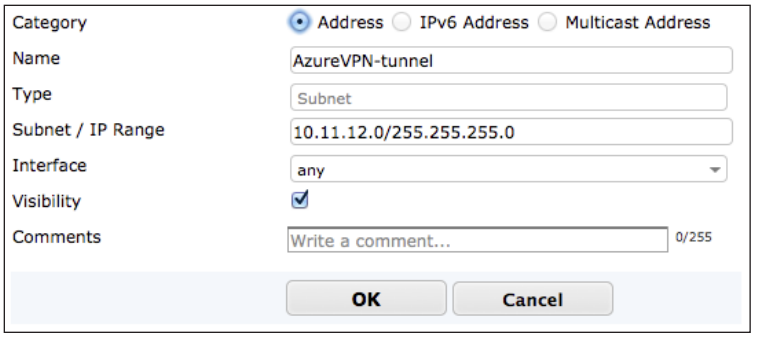



## 4. Creating the FortiGate firewall addresses

Go to **Policy & Objects** > **Objects** > **Addresses** and configure a firewall address for the local network.



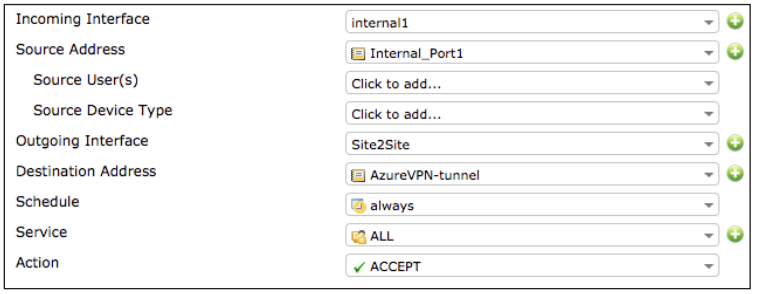
Create another firewall object for the Azure VPN tunnel subnet.




## 5. Creating the FortiGate firewall policies

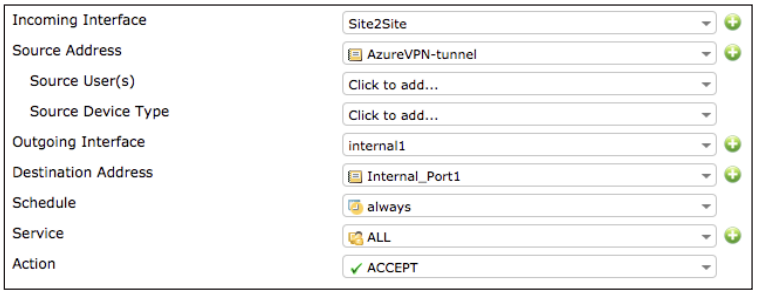
Go to **Policy & Objects** > **Policy** > **IPv4** and create a new policy for the site-to-site connection that allows outgoing traffic.

Set the **Source Address** and **Destination Address** using the firewall objects you just created.



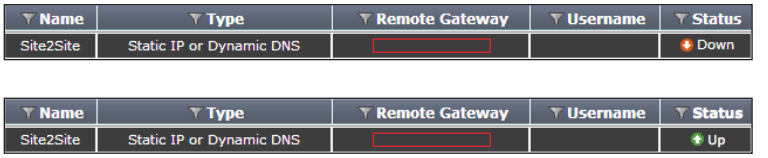

When you are done, create another policy for the same connection to allow incoming traffic.

This time, invert the **Source Address** and **Destination Address**.



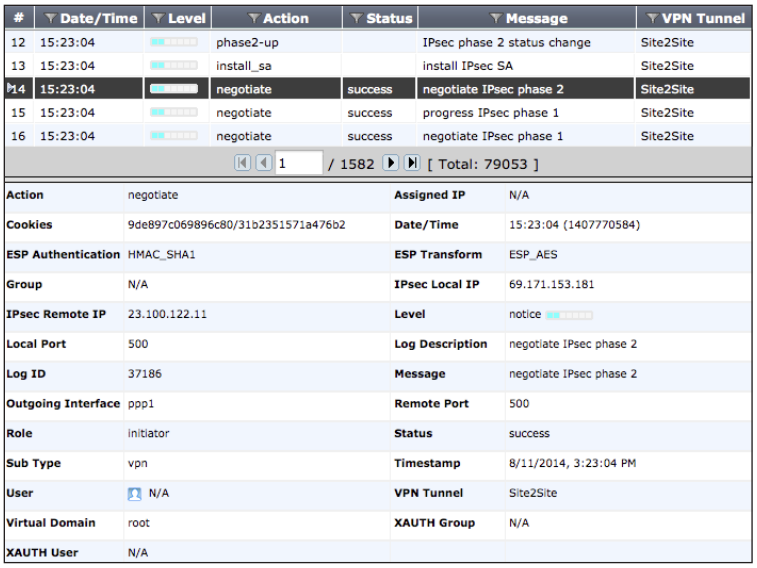

## 6. Results

Go to **VPN** > **Monitor** > **IPsec Monitor**. Right-click the tunnel you created and select **Bring Up** to activate the tunnel.



Go to **Log & Report** > **Event Log** > **VPN**.

Select an entry to view more information and verify the connection.



| # | Date/Time | Level | Action | Status | Message | VPN Tunnel |
|---|---|---|---|---|---|---|
| 12 | 15:23:04 | | phase2-up | | IPsec phase 2 status change | Site2Site |
| 13 | 15:23:04 | | install_sa | | install IPsec SA | Site2Site |
| 14 | 15:23:04 | | negotiate | success | negotiate IPsec phase 2 | Site2Site |
| 15 | 15:23:04 | | negotiate | success | progress IPsec phase 1 | Site2Site |
| 16 | 15:23:04 | | negotiate | success | negotiate IPsec phase 1 | Site2Site |

1 / 1582 [ Total: 79053 ]

| | | | |
|---|---|---|---|
| **Action** | negotiate | **Assigned IP** | N/A |
| **Cookies** | 9de897c069896c80/31b2351571a476b2 | **Date/Time** | 15:23:04 (1407770584) |
| **ESP Authentication** | HMAC_SHA1 | **ESP Transform** | ESP_AES |
| **Group** | N/A | **IPsec Local IP** | 69.171.153.181 |
| **IPsec Remote IP** | 23.100.122.11 | **Level** | notice |
| **Local Port** | 500 | **Log Description** | negotiate IPsec phase 2 |
| **Log ID** | 37186 | **Message** | negotiate IPsec phase 2 |
| **Outgoing Interface** | ppp1 | **Remote Port** | 500 |
| **Role** | initiator | **Status** | success |
| **Sub Type** | vpn | **Timestamp** | 8/11/2014, 3:23:04 PM |
| **User** | N/A | **VPN Tunnel** | Site2Site |
| **Virtual Domain** | root | **XAUTH Group** | N/A |
| **XAUTH User** | N/A | | |

Return to the Microsoft Azure virtual network **Dashboard**. The status of the tunnel will show as **Connected**.

**Data In** and **Data Out** will indicate that traffic is flowing.